NIST National Institute of Standards and Technology • U.S. Department of Commerce
INFORMATION TECHNOLOGY LABORATORY
NO. 103 August 2008

ITL SEEKS NEW CRYPTOGRAPHIC HASH ALGORITHM FAMILY

To help federal agencies protect their information and information systems, ITL is seeking candidates for a new and robust cryptographic hash algorithm. The new hash algorithm is needed because of recent advances in the cryptanalysis of hash functions.

The new algorithm, to be named SHA-3, will augment the hash algorithms currently specified in Federal Information Processing Standard (FIPS) 180-2, *Secure Hash Standard*. In a *Federal Register* notice (Vol. 72, No. 212, pp. 62212-20) published on November 2, 2007, ITL invited interested parties to submit nominations, and provided the nomination requirements and the minimum acceptability requirements for the new algorithm. The notice also included the evaluation criteria that will be used to assess the nominations. The *Federal Register* notice is available at http://www.csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf.

Hash algorithms accept potentially large variable size input messages and produce a small (generally in the range of 160- to 512-bit) fixed-size output called a hash value or message digest, which is a condensed representation of the electronic data in the message. Hash functions are used as building blocks in many cryptographic algorithms and processes. Many algorithms and processes that provide a security service use a hash function as a component of the algorithm or process, including keyed hash message authentication code (HMAC), digital signatures, key derivation functions, and random number generators. In a digital signature application, the hash value of the message is signed instead of the message itself; the signature can later be used to verify the message signer as well as the integrity of the signed message.

ITL issued the federal government's first hash standard in 1993 as FIPS 180, *Secure Hash Standard*, which specified the hash algorithm SHA-0. This standard was revised and issued as FIPS 180-1 in 1995 and as FIPS 180-2 in 2002. These revisions replaced the original SHA-0 with more secure algorithms: the 160-bit SHA-1 and the SHA-2 family of hash functions, which includes SHA-224, SHA-256, SHA-384, and SHA-512 where the suffix indicates the size of the message digest.

Recently, cryptanalysts have found ways to attack several commonly used hash functions, and vulnerabilities have been published on SHA-1. Although no practical attacks have been successful to date against SHA-1, ITL decided that a new hash algorithm is needed to augment the hash algorithms that are currently available and to provide strengthened security for digital signature and other applications for future years.

ITL must receive all candidate nominations of new hash algorithms **by October 31, 2008**. For more information, see http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.

Preview of Online Digital Library of Mathematical Functions

ITL has released a five-chapter preview of the NIST Digital Library of Mathematical Functions (DLMF) for public comment. The online digital library is designed to be the definitive reference work on the special functions of applied mathematics. Special functions are "special," because they occur very frequently in the mathematical modeling of physical phenomena, from atomic physics to water waves. Some of these functions have also found application in areas such as cryptography and signal analysis. The DLMF provides basic information needed to use such functions in practice, such as their definitions, alternate mathematical representations, extreme values, and relationships between functions. It provides various visual aids to provide qualitative information on the behavior of mathematical functions, including interactive Web-based tools for rotating and zooming in on three-dimensional representations. Also provided is advice on methods for computing such functions, as well as pointers to available software.

The DLMF is designed to be a modern successor to the *Handbook of Mathematical Functions* (M. Abramowitz and I. Stegun, Eds.), which was originally published by NIST in 1964. With an estimated one million copies in print, the handbook is the most widely distributed NIST publication in the Institute's 107-year history. And, with more than 1,600 yearly citations in the research literature in recent years, the handbook remains among the most cited works in the mathematical literature.

The Preview Edition of the DLMF contains five chapters: "Gamma Function," "Airy & Related Functions," "Functions of Number Theory," "3j, 6j, 9j Symbols," and "Asymptotic Approximations." It can be accessed at http://dlmf.nist.gov/.

The complete DLMF, with 31 additional chapters providing information on mathematical functions from Bessel to Zeta, is expected to be released in early 2009. A print edition that contains an approximately 1,000-page subset of the information available online will also be published. The DLMF, which is being compiled and extensively edited at NIST, is the

If you are interested in receiving our newsletter, send your name, organization, and business mailing address to:

ITL Newsletter
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

You will be placed on this mailing list only.

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of new information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
E-mail: elizabeth.lennon@nist.gov

result of contributions of more than 50 subject-area experts worldwide. The NIST Editors for the DLMF are Frank Olver, Daniel Lozier, and Ronald Boisvert of the ITL Mathematical and Computational Sciences Division, and Charles Clark of the Physics Laboratory, Electron and Optical Physics Division.

FEDERAL INFORMATION PROCESSING STANDARD (FIPS) ACTIVITIES

On July 29, 2008, a *Federal Register* notice announced the approval of FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, which is a revision of FIPS 198. The FIPS specifies a mechanism for message authentication using cryptographic hash functions in federal information systems. FIPS 198-1 removed the technical information that was included in the previous version that may need frequent updating, such as the security provided by the HMAC algorithm and HMAC values. This change enables ITL to employ a more effective process for keeping the technical information current. Currently, ITL provides the removed technical information and other related important technical details about the HMAC algorithm in NIST Special Publication 800-107, DRAFT *Recommendation for Applications Using Approved Hash Algorithms*, which can be updated in a timely manner as technical conditions change. FIPS 198-1 is available at http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf.

NEW PUBLICATIONS

ITL has launched a new publications database to make it easier for our customers to locate and access our documents. The new database allows searches by author, title, keyword, division, journal name, research area, and date parameters. The website is http://www.itl.nist.gov/publications/publications.cgi.

Guide to SSL VPNs
By Sheila Frankel, Paul Hoffman, Angela Orebaugh, and Richard Park
NIST Special Publication (SP) 800-113
July 2008
http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf

In planning a virtual private network (VPN) deployment, many organizations are faced with a choice between an IPsec-based VPN and a Secure Sockets Layer (SSL)-based VPN. This document seeks to assist organizations in understanding SSL VPN technologies. The publication also makes recommendations for designing, implementing, configuring, securing, monitoring, and maintaining SSL VPN solutions. SP 800-113 provides a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also includes a comparison with other similar technologies such as Internet Protocol Security (IPsec) VPNs and other VPN solutions.

Performance Measurement Guide for Information Security
By Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson
NIST Special Publication 800-55 Revision 1
July 2008
http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective measurement program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans
By Ron Ross, Arnold Johnson, Stu Katzke, Patricia Toth, Gary Stoneburner, and George Rogers
NIST Special Publication 800-53A
June 2008
http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf

This document provides guidelines for building effective security assessment plans and procedures to enable the assessment of security controls

employed in information systems supporting the executive agencies of the federal government. Organizations should use this publication in conjunction with an approved system security plan to create a viable security assessment plan for producing and compiling the information necessary to determine the effectiveness of the security controls employed within the information system.

VVSG Companion Document for the Election Official Community
By John Wack
NISTIR 7488
March 2008
http://vote.nist.gov

This document is an overview to the Voluntary Voting System Guidelines (VVSG) recommendations to the Election Assistance Commission (EAC) of August 31, 2007. It summarizes major topics in the security, human factors, and core requirements of voting systems and focuses primarily on topics that are new or that represent significant changes from the VVSG 2005. Tutorials on the guidelines are also available.

Operational Measures and Accuracies of ROC Curve on Large Fingerprint Data Sets
By Jin Chu Wu
NISTIR 7495
May 2008
http://www.itl.nist.gov/iad/894.03/

This report describes research on large fingerprint data sets. At any point on a receiver operating characteristic (ROC) curve in combination with two distributions of genuine scores and impostor scores, there are three related variables: the true accept rate (TAR) of the genuine scores, the false accept rate (FAR) of the impostor scores, and the threshold. Any one of these three variables determines the other two variables. The measures and accuracies of TAR and threshold while FAR is specified, and the measures and accuracies of TAR and FAR once threshold is fixed, are all investigated. In addition, the measures and accuracies of the equal error rate (EER) and the corresponding threshold are also explored.

Usability Testing of Height and Angles of Ten-Print Fingerprint Capture
By Mary Theofanos, Brian Stanton, Charles Sheppard, Ross Micheals, Nien-Fan Zhang, John Wydler, Larry Nadel, and William Rubin
NISTIR 7504
June 2008
http://zing.ncsl.nist.gov/biousa/

This paper describes a study for the Department of Homeland Security that examined the impact on the time required to collect fingerprints and the quality of fingerprint images when fingerprint scanners are angled at tall counters to accommodate a broader range of visitors. Sloping of the fingerprint scanner had no impact on user performance.

MARK YOUR CALENDAR

2008 Security Automation Conference and Workshop (4th Annual)
Dates: September 23-24, 2008 (workshops September 22 and 25, 2008)
Place: NIST, Gaithersburg, Maryland
Registration fee: $95
Sponsors: NIST, NSA, DISA, DHS

This conference will focus on the use of specific open standards to enable security automation in government and private industry; vulnerability and security configuration management; impact analysis for emerging security issues; and policy compliance verification. Topics will include public-private partnerships and government collaborations, and the Information Security Automation Program (ISAP). The target audience is security managers and staff, security content tool vendors, IT products vendors, testing laboratories, and auditors.

NIST technical contact: Stephen Quinn, 301/975-6967, stephen.quinn@nist.gov
Conference website: http://nvd.nist.gov/events.cfm

Biometric Consortium Conference 2008 (BC2008)
Dates: September 23-25, 2008
Place: Tampa, Florida
Registration fee: $595/$695
Sponsors: NIST, NSA, DHS, Biometrics Task Force, NIJ, GSA, Volpe Center, AFCEA

This conference will focus on utilizing biometric-based solutions for a wide range of personal identification/authentication applications including homeland security and the prevention of identity theft. The target audience is policy developers and decision makers, government and industry executives, information technology (IT) users and developers, IT Chief Executive Officers, Chief Technical Officers and product managers, law enforcement officials, system integrators, personal authentication and information security specialists, educators and students, government, industry, and academia researchers.

NIST technical contact: Fernando Podio, 301/975-2947, fernando.podio@nist.gov
Conference website: http://www.biometrics.org/BC2008/index.htm

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.